Chapter 17 - National Security Information Policies

1701 Purpose

The Department of Commerce Security Manual prescribes the policies, procedures, and standards that govern the safeguarding of classified national security information. Section III of the Security Manual implements Executive Order (E.O.) 12958, Classified National Security Information, and establishes a system for classifying, declassifying, and downgrading national security information. Section III also provides guidance for the enforcement and management of security responsibilities and the procedures for reporting, reviewing, and recording security infractions and violations. The provisions of this section set forth the minimum security standards and safeguards to ensure protection of national security information in the Department of Commerce.

1702 Application

A. In a Presidential Document signed October 13, 1995, the President of the United States conferred classification authority on the Secretary of Commerce to originally classify information at the Secret classification level. Departmental Organization Order (DOO) 20-6 designates the Director for Security as the "senior agency official" to direct and administer the Department of Commerce national security information program implementing E.O. 12958, under which information is classified, safeguarded, and declassified.

B. The national security information policies, procedures, and standards prescribed in this section apply to employees and applicants for employment with the Department as well as contractors, guest researchers, committee members, students and trainees, and other persons designated by the Secretary of Commerce for access to classified information. In addition, senior managers, supervisors, and employees are responsible for familiarization and compliance with all personnel security regulations and procedures at their respective installations.

C. Questions concerning policies pertaining to national security information should be referred to the Office of Security through the servicing security officer. Policy interpretations should be addressed to the Office of Security. The Director for Security shall provide the Department's interpretation of policies and procedures concerning the protection of national security information, and, as necessary, provide written guidance to operating units and other departmental offices.

1703 National Security Information Policies

Policies for the Department's National Security Information program are outlined below.

A. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life. Our national interest requires that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Accordingly, classifying authorities, program managers, supervisors, and employees shall follow the provisions of Executive Order 12958, Classified National Security Information, or subsequent orders, to protect national security information.

B. Our nation's democratic principles also require that the American people be informed of the activities of their Government; therefore, information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. If there is significant doubt about the need to classify information, the information shall not be classified. If the classifying authority has a significant doubt about the appropriate level of classification, he or she will classify the information at the lower level. In addition, classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

C. The authority to classify original information at the Secret or Confidential level may be exercised only by the Secretary of Commerce and officials to whom Original Classification Authority (OCA) has been delegated. No departmental official is authorized to classify original information at the Top Secret level. Officials authorized to classify information at the Secret level are also authorized to classify information at the Confidential level.

D. The delegation of original classification authority will be limited to the minimum number of individuals absolutely required for the efficient administration and protection of programs in the Department. Classification authority delegated by the Secretary cannot be re-delegated but may be exercised by persons designated in writing to act in the absence of the designated classifying authority, provided they have the appropriate level of security clearance.

E. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. With the appropriate security clearance, Department of Commerce employees involved in the production or generation of information based on previously classified information are authorized to derivatively classify information.

F. E.O. 12958 encourages authorized holders of classified information to challenge classification decisions as a means of promoting proper and thoughtful classification actions. Authorized holders wishing to challenge the

classification status of information shall present such challenges to a classification authority who has jurisdiction over the information. A formal challenge under this provision shall be in writing and coordinated with the Office of Security.

G. Information that continues to meet the classification requirements of E.O. 12958, or subsequent orders, requires continued protection; however, Department of Commerce information shall be declassified as soon as it no longer meets the standards for classification under this Executive Order. When classified information is transferred from another agency or operating unit in conjunction with a transfer of functions, and not merely for storage purposes, the receiving operating unit shall be deemed to be the originating office for purposes of downgrading and declassification.

H. Each operating unit that holds classified information shall establish and implement procedures for systematic declassification. This program shall apply to historically valuable records exempted from automatic declassification under E.O. 12958. Operating units shall prioritize the systematic review of records based upon the degree of researcher interest and the likelihood of declassification upon review. Operating units or offices shall maintain a current listing of officials delegated declassification authority by name, position, or other identifier. If possible, this listing shall be unclassified.

I. Unless properly exempted from automatic declassification, all classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under Title 44 of the U.S. Code, shall be automatically declassified whether or not the records have been reviewed.

J. Classified information under Department of Commerce jurisdiction must be reviewed for declassification upon receipt of a request by a United States citizen or permanent resident alien, a Federal agency, or a state or a local government. A request for mandatory review of classified information shall be submitted in writing and describe the information with sufficient specificity to locate it with a reasonable amount of effort.

K. The head of an office shall appoint, in writing, an appropriately cleared employee to serve as the Top Secret and Secret Control Officer within his or her operating unit. The Top Secret or Secret Control Officer is responsible for receiving, dispatching, and maintaining control and accountability of Top Secret or Secret information within their unit. Top Secret and Secret Control Officers shall inventory Top Secret and Secret documents on an annual basis, or more frequently where circumstances warrant.

L. The head of each operating unit must establish procedures for the control and accountability of Top Secret, Secret, and Confidential information by use of written records or an electronic database. Each operating unit shall designate an office/unit Classified Control Point. Exceptions may be requested by the operating unit.

Procedures shall ensure that the movement of classified information can be traced, its dissemination is limited, the retrieval of information can be obtained promptly, the loss of information can be detected, and excessive holdings and reproduction are limited. Offices maintaining classified information must conduct an annual inventory and review their classified holdings. Each document must be visually inspected upon initial receipt and during the annual inventory to ensure that the document is complete or accounted for by written evidence of proper disposition. This inventory shall include a review to determine possible downgrade, declassification, or destruction of classified holdings to reduce the amount necessary for operational and program purposes. The results of this inventory shall be forwarded to the Office of Security through the security contact or servicing security officer.

M. Federal employees are not automatically cleared for access to classified information. The number of personnel cleared and granted access to classified information in the Department should be maintained at the minimum number consistent with operational requirements and needs. When a person no longer needs access to a particular security classification level, the security clearance should be adjusted, or downgraded, to the classification level required for the performance of the person's official duties and obligations. The administrative downgrade or withdrawal of an individual's security clearance does not prejudice the person's eligibility for a future security clearance.

N. No employee has a right to gain access to classified information solely by virtue of title, position, or level of security clearance. An employee is eligible for access to classified information provided the employee has been determined to be trustworthy by the appropriate investigation and access is essential to accomplish lawful and authorized Government purposes.

O. Classified information (in any form), to include extra copies, is not personal property and may not be removed from the Government's control by any departing official. The head of each operating unit shall ensure that all separating personnel account for all classified information in their possession and transfer all classified material to an authorized custodian.

P. Heads of operating units must ensure that only authorized persons obtain access to classified information; however, the final responsibility for determining whether an individual obtains access to classified information rests with the individual who has possession, knowledge, or control of the information and not with the prospective recipient. Classified information must be protected at all times by the holder of the information. Before classified information is disclosed, the holder must verify the recipient's identification and security clearance through their operating unit's servicing security officer or security contact, determine the recipient's need to know, and advise the recipient of the classification level of the information.

Q. Classified information may be transmitted by authorized means both inside and outside of the Department; however, classified information may be hand-carried aboard commercial passenger aircraft only when there is neither time nor means available to properly transmit the information by other authorized means. The Director for Security may grant permission to carry classified material overseas on a case-by-case basis. Requests for permission to carry classified information aboard a commercial passenger aircraft shall be submitted in writing to the Office of Security by the servicing security officer no less than ten working days prior to departure.

R. Servicing security officers may authorize an employee to hand-carry classified information up to the Top Secret level within the United States and its territories, except by commercial aircraft. This authorization is required for employees who routinely carry classified material to facilities in the same geographical areas. To be an authorized courier, the employee must hold an appropriate security clearance and possess a valid Courier Authorization Card, CD-75, as described in paragraph 2207 of the Security Manual.

S. Classified information must be stored under conditions that will provide adequate protection against access by unauthorized persons. Whenever classified information is not under the personal control and observation of a cleared person, it must be guarded by personnel with the appropriate security clearance or stored in a locked GSA-approved security container. An office that receives classified information (in any form) and has no authorized storage equipment available must either return the classified information to the sender, arrange with another office to properly store the information, or destroy it by an approved method. Under no circumstances shall classified information be left unattended, in an unauthorized storage container, or in the custody of a person who does not have the proper security clearance and an established need-to-know.

T. The head of an operating unit or the servicing security officer may determine that more stringent requirements are needed based on the volume, nature, and sensitivity of the information to be protected in relation to other factors such as types of containers, presence of guards, vault-type space, or intrusion alarms. Bulky Secret and Confidential information may be stored in vaults or other closed areas that have been approved and accredited for this purpose by the Office of Security; however, no area shall be used for classified open storage without prior accreditation and written approval from the Office of Security.

U. The head of each operating unit responsible for protecting classified information will develop and implement procedures to protect incoming mail, bulk shipments, and items delivered by messenger that contain classified material. Procedures shall be established at receipt points to limit access to classified information to cleared personnel only.

V. Classified documents shall be destroyed in a manner sufficient to preclude recognition or reconstruction of the classified information. The heads of operating units shall ensure that procedures are established for the

proper destruction of classified information in their operating unit. Such procedures must ensure that adequate destruction records are maintained, authorized destruction methods are used, information is protected during transport, and the destruction is properly witnessed. Classified documents may be destroyed only by authorized methods.

W. Classified National Security Information shall not be discussed over, or otherwise transmitted or processed by, any form of telecommunications unless approved measures are taken to protect the information. Basic policies dealing with the security of Federal telecommunications are developed and issued under the purview of the National Security Council. Implementing instructions are issued by the National Security Agency (NSA). The Department of Commerce Security Manual implements the NSA security requirements governing communications security equipment and operations. In addition, operating systems processing classified national security information shall be reviewed every three years for certification and accreditation or when major changes are made to the system.

X. All security incidents, violations, or compromises must be reported through the servicing security officer to the Office of Security headquarters. Any person who has knowledge or suspects the loss or possible compromise of classified information (in any media), or any person who discovers classified information out of proper control, to include classified information discovered improperly safeguarded and left unattended and unsecured, shall immediately take custody of such information and safeguard it in an appropriate manner and report the loss or possible compromise to their security contact, servicing security officer, or the Office of Security.

Y. Each security violation or infraction shall be noted on the employee's performance evaluation, may result in a review of security clearance retention, and shall be referred to the operating unit to determine if disciplinary action is warranted. Based on a security violation reported and validated on a CD-349, Report of Security Violation, the Office of Security will recommend that the employee's immediate supervisor issue a written reprimand to an employee responsible for the security violation or three security infractions within a 12-month period. If an individual has acquired fewer than three infractions within a 12-month period, but the servicing security officer deems any or all of the infractions to be sufficiently serious, the security officer may recommend appropriate disciplinary action through the Office of Security to the head of an operating unit, citing the infractions as an indicator of a more serious problem.

Z. Security contacts, servicing security officers, and cleared Office of Security personnel are responsible for conducting random after-hours inspections to ensure that classified information is properly protected and secured. Persons participating in these official inspections are authorized to enter any office under the actual control and/or possession of the Department of Commerce and/or any subordinate operating unit at any time.

Designated security personnel are authorized to conduct such inspections in the performance of their official duties. This inspection may consist of a search of desktops, desk drawers, cabinets or other miscellaneous office furniture and equipment within the confines of a government-owned or leased building utilized by Department or operating unit personnel. The purpose of the inspection is to ensure that classified and critically sensitive information is being protected properly. Inspections involving Department of Commerce office space occupied by employees of, or under the control of, another agency shall be coordinated with the other agency.

1704 Statutory Requirements

A. Nothing in these regulations shall be construed as authorizing the dissemination, handling, or transmission of information contrary to the provisions of any statute. In any conflict, specific statutory provisions shall prevail.

B. Invention Secrecy Act.

1. **Classified Patent Documents**. Patent applications and certain related documents are subject to the Invention Secrecy Act of 1951, as amended (35 U.S.C. §§ 181-188), which concerns the secrecy of certain inventions and related matters. These documents may contain information identified as national security information. When such documents contain classified information, they must be safeguarded in accordance with the provisions of this section of the United States Code and E.O. 12958 or subsequent orders.

2. **Applications Pending Review.** Patent applications that have not yet been reviewed for security classification should be safeguarded as Confidential national security information until the appropriate authority makes a classification determination.

3. **Unclassified Applications.** Unclassified patent applications that have been imposed with a Type 1 Secrecy Order do not require the safeguards afforded to classified information. These applications and related documents are subject to the export control laws and must be provided adequate protection to prevent access by unauthorized persons (50 U.S.C. § 2401 et seq.). The level of protection is normally less stringent than that required for national security information.

1705 Classified Projects Sponsored by Other Government Agencies

Classified projects undertaken by an operating unit for another Federal Government agency may be carried out either under the security regulations of the sponsoring agency or the Department of Commerce. Specific

security measures will be prescribed when the agreement or contract is made, and there will be no deviation from the agreement thereafter except with mutual consent of both the performing office and the sponsoring organization. When coordinating with other agencies, it is incumbent upon employees of the Department to verify the identification, security clearance, and need-to-know of persons who will have access to classified information under their control. When entering into contractual agreements involving classified information, program managers must notify their servicing security officer.

1706 Procedural Exemptions

A. A request for an exception to the procedural provisions of this section must be made in writing to the Office of Security and must set forth all salient facts, justifications, and a proposed alternate procedure. Some requests for waivers from the provisions of E.O. 12958 or implementing directives cannot be granted at the departmental level. However, the Director for Security will consider such requests and, if approved, will forward the request to the Information Security Oversight Office for a final decision.

B. The Director of the Information Security Oversight Office has determined that restrictions contained in E.O. 12958 do not apply to the use of the term "Confidential" in relation to data collected by the Bureau of the Census. Title 13, United States Code (U.S.C.), enables the Bureau to use the term "Confidential" as a guarantee to citizens of the United States that whatever personal and private information the Bureau collects will be protected from disclosure. Identifying data as "CENSUS Confidential" does not violate the provisions of E.O. 12958 when the term refers to Census information and not to national security information.

1707 Reporting Requirements

A. Original Classification Authority. The Office of Security shall maintain a current list of individuals in the Department by position who have been delegated Original Classification Authority (OCA) and the authority to declassify information. The head of an operating unit or the servicing security officer shall notify the Office of Security when a change occurs regarding delegations of authority within their operating units or servicing areas.

B. Classification Actions. OCAs are responsible for maintaining records concerning original and derivative classification actions made throughout the year. Servicing security officers or security contacts shall establish the means in their respective organizations to obtain the information required by the Information Security Oversight Office (ISOO) concerning original and derivative classification actions made by original classification authorities. Servicing security officers or security contacts shall review records and reports to ensure the information submitted by an OCA is complete and accurate.

C. Inventory of Top Secret and Secret Documents. OCAs will ensure that an inventory of Top Secret and Secret documents is maintained in either written or electronic form in their respective organizations. The Top Secret and Secret control officers shall inventory Top Secret and Secret documents and material at least annually, or more frequently when necessary. During the inventory, each document or item shall be physically reviewed and examined for completeness and accuracy or accounted for by examination of written evidence of proper disposition.

D. Cost Estimates of Classification-related Actions. The heads of operating units will ensure that cost estimates associated with classification-related activities are reported through the servicing security officer to the Office of Security by October 30 for the previous fiscal year. These classification-related activities include personnel security, classification management, electronic security, and other related activities. In addition to costs associated with classification activities, this report requests information concerning costs associated with declassification activities. These costs will be collected by the Office of Security and transmitted directly to the Information Security Oversight Office (ISOO). The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under E.O. 12829, will collect the cost estimates for the classification-related activities of departmental contractors, licensees, and Federal advisory committee members and report those costs to ISOO. ISOO is ultimately responsible for providing a final annual report to the President on these costs.

E. Missing or Compromised Classified Information. An employee who discovers that a classified document is either missing or compromised or believes that a classified document is missing or compromised must verbally report the discovery to the appropriate servicing security officer within 24 hours following the discovery. In the case of a known or suspected compromise of a Top Secret document or special access program information, the servicing security officer must report this information immediately and directly to the Office of Security.

F. Contact with Foreign Nationals.

1. Employees must report contacts with foreign nationals from any country who:

   a. Seek unauthorized access to sensitive or classified information;

   b. Request unclassified or other publicly available information, particularly when there is an offer of exchange or payment of some kind, or if the request involves undue flattery or attention for the service performed; or

c. Display efforts to become friendly, no matter how innocuous;

d. Offer help or assistance in performing duties or accomplishing tasks; or

e. Request the help or assistance of a specific employee outside of routine channels.

2. Employees must report information about this contact within five days of the occurrence through their servicing security officer to the Office of Security. The report shall include:

a. The name, office, and telephone number of the individual making the report and the date the report is submitted;

b. The date and type of contact (business, social, etc.);

c. The foreign national's name and address (business and residential), citizenship, or country;

d. A description of the individual, including the sex, approximate height and weight, color of hair, color of eyes, and other distinguishing features;

e. Whether the contact being reported was the first such contact with the individual, or, if there had been others, the approximate date(s); and

f. A detailed narrative of the incident.

G. Other Security Reports. Each servicing security officer of an operating unit or of an Administrative Support Center or the designated security contacts of other operating units shall submit the reports listed below to the Office of Security at the Herbert C. Hoover Building in Washington, D.C. in a timely manner.

1. **Classification Actions.** Servicing security officers and security contacts shall submit the SF-311, Agency Security Classification Management Program Data, to the Office of Security in Washington, D.C. by October 30 each year. This report covers original and derivative classification actions by an OCA for the period of October 1 through September 30.

2. **Top Secret and Secret Inventory Review.** Organizations maintaining an inventory of Top Secret and Secret documents on an electronic database or in written format will submit a copy of the certified

inventory review by the Top Secret and/or Secret control officer through their servicing security officer to the Office of Security in Washington, D.C., by October 30 each year. The report shall reflect the inventory of Top Secret and Secret documents as of October 1.

3. **Security Violations.** Individuals discovering a security violation or compromise shall submit Report of Security Violation, Form CD-349, to their servicing security officer within five working days of the discovery of the violation.